VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER BERICHT ÜBER DIE PATENTIERBARKEIT

(Kapitel II des Vertrags über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens)

Aktenzeichen des Anmelders oder Anwalts MIF 109WO	**WEITERES VORGEHEN** siehe Formblatt PCT/IPEA/416	
Internationales Aktenzeichen PCT/EP2004/012435	Internationales Anmeldedatum *(Tag/Monat/Jahr)* 03.11.2004	Prioritätsdatum *(Tag/Monat/Jahr)* 10.11.2003
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK G06F12/14		
Anmelder MICRONAS GMBH et al.		

1. Bei diesem Bericht handelt es sich um den internationalen vorläufigen Prüfungsbericht, der von der mit der internationalen vorläufigen Prüfung beauftragten Behörde nach Artikel 35 erstellt wurde und dem Anmelder gemäß Artikel 36 übermittelt wird.
2. Dieser BERICHT umfaßt insgesamt 5 Blätter einschließlich dieses Deckblatts.
3. Außerdem liegen dem Bericht ANLAGEN bei; diese umfassen
   a. ☐ *(an den Anmelder und das Internationale Büro gesandt)* insgesamt Blätter; dabei handelt es sich um
      ☐ Blätter mit der Beschreibung, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit Berichtigungen, denen die Behörde zugestimmt hat (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsvorschriften).
      ☐ Blätter, die frühere Blätter ersetzen, die aber aus den in Feld Nr. 1, Punkt 4 und im Zusatzfeld angegebenen Gründen nach Auffassung der Behörde eine Änderung enthalten, die über den Offenbarungsgehalt der internationalen Anmeldung in der ursprünglich eingereichten Fassung hinausgeht.
   b. ☐ *(nur an das Internationale Büro gesandt)* insgesamt (bitte Art und Anzahl der/des elektronischen Datenträger(s) angeben) , der/die ein Sequenzprotokoll und/oder die dazugehörigen Tabellen enthält/enthalten, nur in computerlesbarer Form, wie im Zusatzfeld betreffend das Sequenzprotokoll angegeben (siehe Abschnitt 802 der Verwaltungsvorschriften).

4. Dieser Bericht enthält Angaben zu folgenden Punkten:

☒	Feld Nr. I	Grundlage des Bescheids
☐	Feld Nr. II	Priorität
☐	Feld Nr. III	Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
☐	Feld Nr. IV	Mangelnde Einheitlichkeit der Erfindung
☒	Feld Nr. V	Begründete Feststellung nach Arikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
☐	Feld Nr. VI	Bestimmte angeführte Unterlagen
☐	Feld Nr. VII	Bestimmte Mängel der internationalen Anmeldung
☐	Feld Nr. VIII	Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
10.06.2005	20.01.2006
Name und Postanschrift der mit der internationalen Prüfung beauftragten Behörde Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter Mezödi, S Tel. +49 89 2399-6092

INTERNATIONALER VORLÄUFIGER BERICHT ÜBER DIE PATENTIERBARKEIT

Internationales Aktenzeichen
PCT/EP2004/012435

Feld Nr. I Grundlage des Berichts

1. Hinsichtlich der **Sprache** beruht der Bericht auf der internationalen Anmeldung in der Sprache, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   ☐ Der Bericht beruht auf einer Übersetzung aus der Originalsprache in die folgende Sprache, bei der es sich um die Sprache der Übersetzung handelt, die für folgenden Zweck eingereicht worden ist:
   - ☐ internationale Recherche (nach Regeln 12.3 und 23.1 b))
   - ☐ Veröffentlichung der internationalen Anmeldung (nach Regel 12.4)
   - ☐ internationale vorläufige Prüfung (nach Regeln 55.2 und/oder 55.3)

2. Hinsichtlich der **Bestandteile*** der internationalen Anmeldung beruht der Bericht auf *(Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt)*:

Beschreibung, Seiten	
1-23	in der ursprünglich eingereichten Fassung
Ansprüche, Nr.	
2-10, 12, 13	in der ursprünglich eingereichten Fassung
1, 11	eingegangen am 23.06.2005 mit Schreiben vom 20.06.2005
Zeichnungen, Blätter	
1/9-9/9	in der ursprünglich eingereichten Fassung

   ☐ einem Sequenzprotokoll und/oder etwaigen dazugehörigen Tabellen - siehe Zusatzfeld betreffend das Sequenzprotokoll

3. ☐ Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:
   - ☐ Beschreibung: Seite
   - ☐ Ansprüche: Nr.
   - ☐ Zeichnungen: Blatt/Abb.
   - ☐ Sequenzprotokoll *(genaue Angaben)*:
   - ☐ etwaige zum Sequenzprotokoll gehörende Tabellen *(genaue Angaben)*:

4. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der diesem Bericht beigefügten und nachstehend aufgelisteten Änderungen erstellt worden, da diese aus den im Zusatzfeld angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2 c)).
   - ☐ Beschreibung: Seite
   - ☐ Ansprüche: Nr.
   - ☐ Zeichnungen: Blatt/Abb.
   - ☐ Sequenzprotokoll *(genaue Angaben)*:
   - ☐ etwaige zum Sequenzprotokoll gehörende Tabellen *(genaue Angaben)*:

* *Wenn Punkt 4 zutrifft, können einige oder alle dieser Blätter mit der Bemerkung "ersetzt" versehen werden.*

Feld Nr. V Begründete Feststellung nach Artikel 35 (2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	4-9,12-13
	Nein:	Ansprüche	1-3,10,11
Erfinderische Tätigkeit (IS)	Ja:	Ansprüche	5,6,12,13
	Nein:	Ansprüche	1-4,7-10,11
Gewerbliche Anwendbarkeit (IA)	Ja:	Ansprüche:	1-13
	Nein:	Ansprüche:	

2. Unterlagen und Erklärungen (Regel 70.7):

siehe Beiblatt

Zu Punkt V.

1 Im vorliegenden Bescheid wird auf folgende Dokumente verwiesen:
D1: US-A-5 095 525 (ALMGREN ET AL) 10. März 1992 (1992-03-10)
D2: EP-A-1 022 659 (PHILIPS INTELLECTUAL PROPERTY & STANDARDS GMBH; KONINKLIJKE PHILIPS EL) 26. Juli 2000 (2000-07-26)

2 UNABHÄNGIGE ANSPRÜCHE 1 UND 11

2.1 Die vorliegende Anmeldung erfüllt nicht die Erfordernisse des Artikels 33(1) PCT, weil der Gegenstand des Anspruchs 1 im Sinne von Artikel 33(2) PCT nicht neu ist. Dokument D2 offenbart (die Verweise in Klammern beziehen sich auf dieses Dokument):

Ein Verfahren zum Speichern von Daten in einem Wahlzugriffsspeicher..., bei dem
- vor der Speicherung eine Verschlüsselung eines jeden Datenwortes erfolgt, indem aus jedem Datenwort ... durch eineindeutiges Permutieren der einzelnen Datenbits unter Verwendung eines ersten Permutationsschlüssels ein permutiertes Datenwort mit der vorgegebenen Anzahl Datenbits erzeugt wird
(Par. 0016,0017), wobei
- der erste Permutationsschlüssel aus einer binären Zufallssequenz erzeugt wird.
(Par. 0020, ein getaktetes rückgekoppeltes Schieberegister ist ein (Pseudo)-Zufallssequenzerzeuger)

2.2 Die vorliegende Anmeldung erfüllt nicht die Erfordernisse des Artikels 33(1) PCT, weil der Gegenstand des Anspruchs 1 nicht auf einer erfinderischen Tätigkeit in Bezug auf D1 im Sinne von Artikel 33(3) PCT beruht. Dokument D1 offenbart (die Verweise in Klammern beziehen sich auf dieses Dokument):

Ein Verfahren zum Speichern von Daten in einem Wahlzugriffsspeicher..., bei dem
- vor der Speicherung eine Verschlüsselung eines jeden Datenwortes erfolgt, indem aus jedem Datenwort ... durch eineindeutiges Permutieren der einzelnen Datenbits unter Verwendung eines ersten Permutationsschlüssels ein permutiertes Datenwort mit der vorgegebenen Anzahl Datenbits erzeugt wird

(Spalte 6, Zeilen 28 - 41)

Der Gegenstand des Anspruchs 1 unterscheidet sich daher von dem bekannten Verfahren dadurch, daß der erste Permutationsschlüssel aus einer binären Zufallssequenz erzeugt wird.

Es ist jedoch fachüblich, Schlüssel automatisch aus Zufallszahlen zu erzeugen. Der Fachmann würde ein solches Merkmal in das Verfahren aus D1 aufnehmen und so ohne erfinderische Tätigkeit zu einem Verfahren gemäß Anspruch 1 gelangen.

2.3 Die Merkmale des unabhängigen Vorrichtungsanspruchs 11 entsprechen im wesentlichen denen des Verfahrensanspruchs 1, dementsprechend gilt für diesen ebenfalls obiger Einwand.

3 ABHÄNGIGE ANSPRÜCHE

Die abhängigen Ansprüche 2 - 4 und 7 - 10 enthalten keine zusätzlichen Merkmale, die in Kombination mit den Merkmalen irgendeines Anspruchs, auf den sie rückbezogen sind, die Erfordernisse in bezug auf Neuheit bzw. erfinderische Tätigkeit erfüllen, da es sich entweder um Merkmale handelt, die aus D1 oder D2 bekannt oder aber fachüblich sind.

Geänderter Patentanspruch 1

1. Verfahren zum Speichern von Daten in einem Wahlzugriffsspeicher, in dem Datenworte, die jeweils eine vorgegebene Anzahl Datenbits umfassen, abspeicherbar sind,
d a d u r c h g e k e n n z e i c h n e t, dass
vor der Speicherung eine Verschlüsselung eines jeden Datenwortes (M) erfolgt, indem aus jedem Datenwort (M) oder einem aus dem Datenwort (M) abgeleiteten Datenwort durch eineindeutiges Permutieren der einzelnen Datenbits (M[n-1]-M[0]) unter Verwendung eines aus einer binären Zufallssequenz erzeugten ersten Permutationsschlüssels (P), ein permutiertes Datenwort (Mp) mit der vorgegebenen Anzahl Datenbits erzeugt wird.

Geänderter Patentanspruch 11

11. Vorrichtung zur Verschlüsselung/Entschlüsselung eines Datenbits (M[n-1], M[k], M[0]) umfassenden Datenwortes (M), die eine Permutationseinheit (14) mit folgenden Merkmale aufweist:

- Dateneingänge zur Zuführung der Datenbits (M[n-1], M[k], M[0]) des zu permutierenden Datenwortes (M),

- Ausgänge zur Bereitstellung der Datenbits (Mp[n-1], Mp[k], Mp[0]) eines permutierten Datenwortes (Mp) der vorgegebenen Länge (n),

- Permutationsschlüsseleingänge zur Zuführung eines Permutationsschlüssels (P), der eine der Anzahl der Datenbits entsprechende Anzahl (n) Teilschlüssel (P[n-1]... P[0]) umfasst,

- einen Signalgenerator (13) der den Permutationsschlüssel (P) aus einer binären Zufallssequenz (RS) erzeugt.

- eine der Anzahl der Datenbits entsprechende Anzahl Auswahleinheiten (14_n-1, 14_k, 14_0), denen jeweils ein Teilschlüssel zugeordnet ist und die jeweils ein Datenbit (Mp[n-1], Mp[k], Mp[0]) des permutierten Datenwortes (Mp) nach Maßgabe je eines der Teilschlüssel (P[n-1]... P[0]) aus den Datenbits des zu permutierenden Datenwortes (M) bereitstellen.